

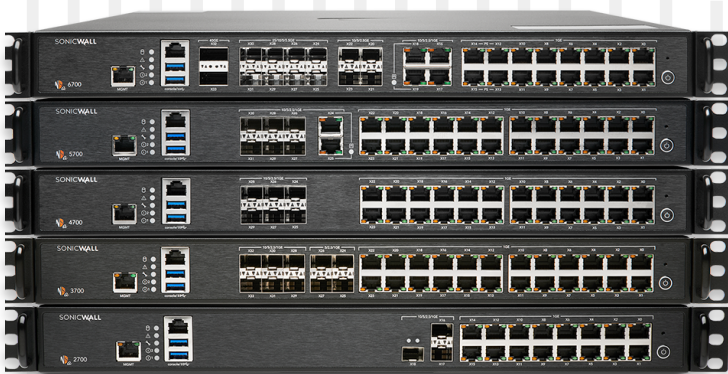
# SonicWall 7세대 NSa 시리즈

SonicWall 7세대(Gen 7) 네트워크 보안 어플라이언스(NSa) 차세대 방화벽(NGFW)은 중간 규모부터 대규모 기업에 동급 최저 총 소유 비용으로 업계 최고 성능을 제공합니다.

침입 방지, VPN, 애플리케이션 컨트롤, 맬웨어 분석, URL, 필터링, DNS 보안, GEO IP, 봇넷 서비스 등 포괄적인 보안 기능을 갖춰, 네트워크 전반을 병목현상 없이 고도화된 위협으로부터 보호합니다.

## 주요 사항

- 1 RU - 폼 팩터
- 40G/25G/10G/5G/2.5G/1G 포트 지원
- 멀티 기가비트급 위협 및 맬웨어 분석 처리량
- 뛰어난 TLS 성능 (세션 및 처리량)
- 확장 가능한 스토리지
- DNS 보안
- 평판 기반의 콘텐츠 필터링 서비스(CFS 5.0)
- Wi-Fi 6 방화벽 관리
- Aruba ClearPass와 네트워크 액세스 제어 통합
- 엔터프라이즈급 인터넷 엣지 지원
- 최신 7세대 SonicOS 지원
- 보안 SD-WAN 기능
- 직관적인 사용자 인터페이스와 중앙집중식 관리
- TLS 1.3 지원
- 동급 최고의 가격대 성능비
- SonicWall Capture Labs 위협 연구팀 제공
- 높은 포트 확장성으로 손쉬운 네트워크 구성
- SonicWall Switch, SonicWave 액세스 포인트 및 Capture Client 통합
- 이중화 전원



7세대 NSa 시리즈 사양 간략 소개. [전체 사양 보기](#) »

최대  
19Gbps

위협 방지  
처리량

최대  
8백만

연결

40G/25G/10G/  
5G/2.5G/1G

포트

높은 포트 확장성을 자랑하고 여러 개의 40GbE 및 10GbE 포트를 갖추고 있으며, 네트워크 및 하드웨어 이중화와 듀얼 전원 공급 장치를 지원하여 고가용성을 보장합니다.

SonicWall 7세대(Gen 7) 네트워크 보안 어플라이언스(NSa) 차세대 방화벽(NGFW)은 중간 규모부터 대규모 기업에 동급 최저 총 소유 비용으로 업계 최고 성능을 제공합니다.

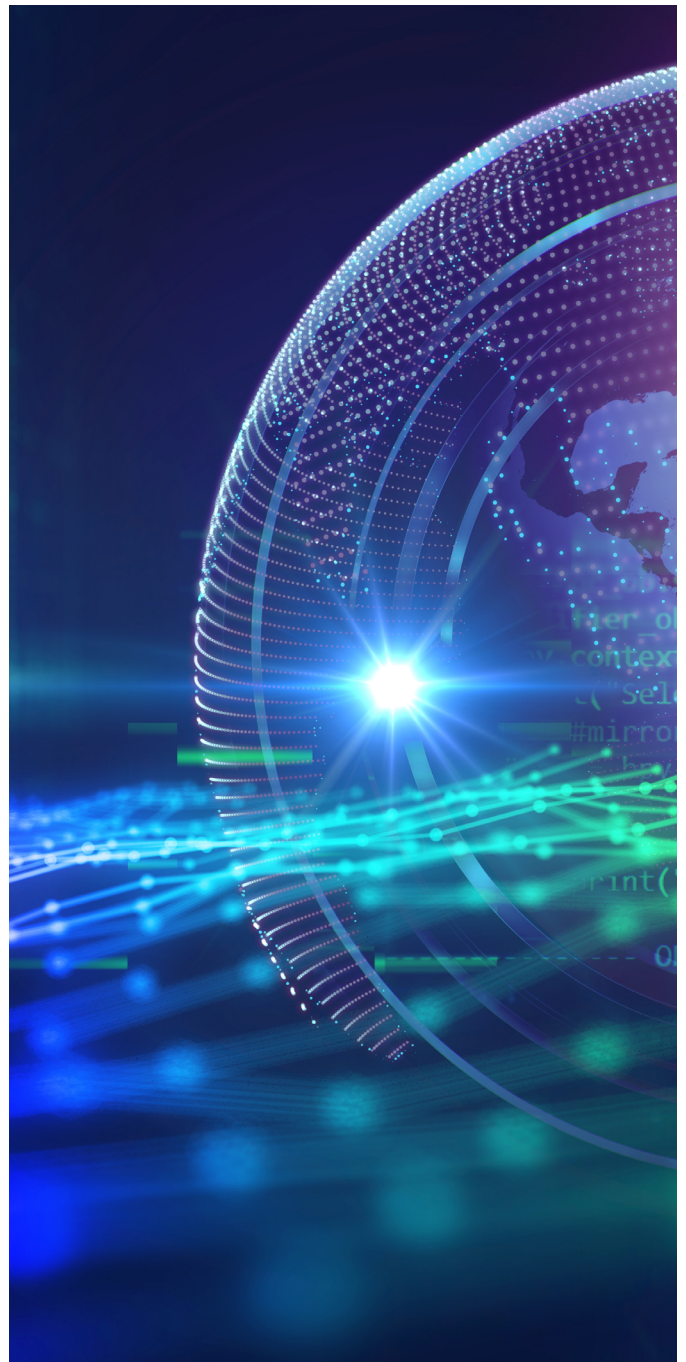
침입 방지, VPN, 애플리케이션 컨트롤, 맬웨어 분석, URL, 필터링, DNS 보안, GEO IP, 봇넷 서비스 등 포괄적인 보안 기능을 갖춰, 네트워크 전반을 병목현상 없이 고도화된 위협으로부터 보호합니다.

7세대 NSa 시리즈는 최신 하드웨어 구성 요소를 기반으로 설계되어 멀티 기가비트급 위협 방지 처리량을 자랑하며, 암호화된 트래픽도 문제없습니다. 높은 포트 확장성을 자랑하고 여러 개의 40GbE 및 10GbE 포트를 갖추고 있으며, 네트워크 및 하드웨어 이중화와 듀얼 전원 공급 장치를 지원하여 고가용성을 보장합니다.

### 7세대 – SonicOS 7 및 보안 서비스

7세대 NSa 시리즈에는 최신 사용자 인터페이스, 직관적인 워크플로, 사용자 우선 설계 원칙을 기반으로 새롭게 설계된 운영 체제인 SonicOS 7.0이 탑재되어 있습니다. SonicOS 7은 엔터프라이즈급 워크플로를 원활히 처리할 수 있도록 설계된 다양한 기능을 제공합니다. 손쉬운 정책 구성, 제로 터치 구축, 유연한 관리를 모두 제공하여 기업이 보안과 운영 효율성을 동시에 향상시킬 수 있습니다.

7세대 NSa 시리즈는 SD-WAN, 동적 라우팅, 4~7레이어 고가용성, 고속 VPN 등 고급 네트워킹 기능을 지원합니다. 이 어플라이언스는 방화벽과 스위치 기능이 통합되어 있으며, 단일 인터페이스로 스위치와 액세스 포인트를 모두 관리할 수 있습니다.



오늘날, 그리고 미래의 고도화된 사이버 공격을 효과적으로 방어할 수 있게 설계된 7세대 NSa 시리즈를 도입하면 수준 높은 SonicWall 방화벽 보안 서비스를 이용하여 귀사의 IT 인프라 전체를 보호할 수 있습니다. 클라우드 애플리케이션 보호, Capture 고급 위협 보호(ATP), 클라우드 기반 샌드박스, 특허받은 실시간 심층 메모리 검사(RTDMI™), 비재조립 심층 패킷 검사(RFDPI) 등의 솔루션과 서비스가 포괄적인 게이트웨이 보호를 제공하여 TLS 1.3를 포함한 모든 트래픽에서 제로데이 및 암호화된 위협 등, 가장 은밀하고 위험한 맬웨어도 차단할 수 있습니다.

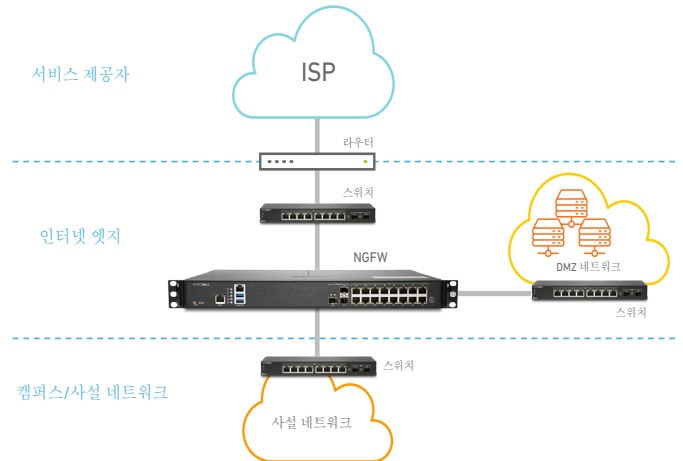
## 구축시 장점

7세대 NSa 시리즈는 중간 규모 분산형 기업에 적합한 두 가지 구축 옵션을 갖추고 있습니다.

### 인터넷 엣지 구축

7세대 NSa 시리즈 NGFW 표준 배포 옵션은 인터넷에서 유입되는 악성 트래픽으로부터 사설 네트워크를 보호합니다. 이 배포 옵션의 특징은 다음과 같습니다.

- 동급 최고 성능, 최고 포트 확장성(40GbE 및 10GbE 연결 포함)을 자랑하는 검증된 NGFW 솔루션 구축
- TLS 1.3 등 암호화된 트래픽에 대한 가시성 확보 및 검사, 인터넷에서 유입되는 침해적 위협을 성능 저하 없이 차단
- 멀웨어 분석, 클라우드 앱 보안, URL, 필터링, 평판 서비스 등 통합 보안으로 기업을 안전하게 보호
- 고급 보안 및 네트워킹 기능이 포함되어 공간과 비용을 절약할 수 있는 통합 NGFW 솔루션
- 직관적인 단일 사용자 인터페이스를 통한 중앙집중식 관리 시스템으로 복잡성을 해소하고 효율 극대화

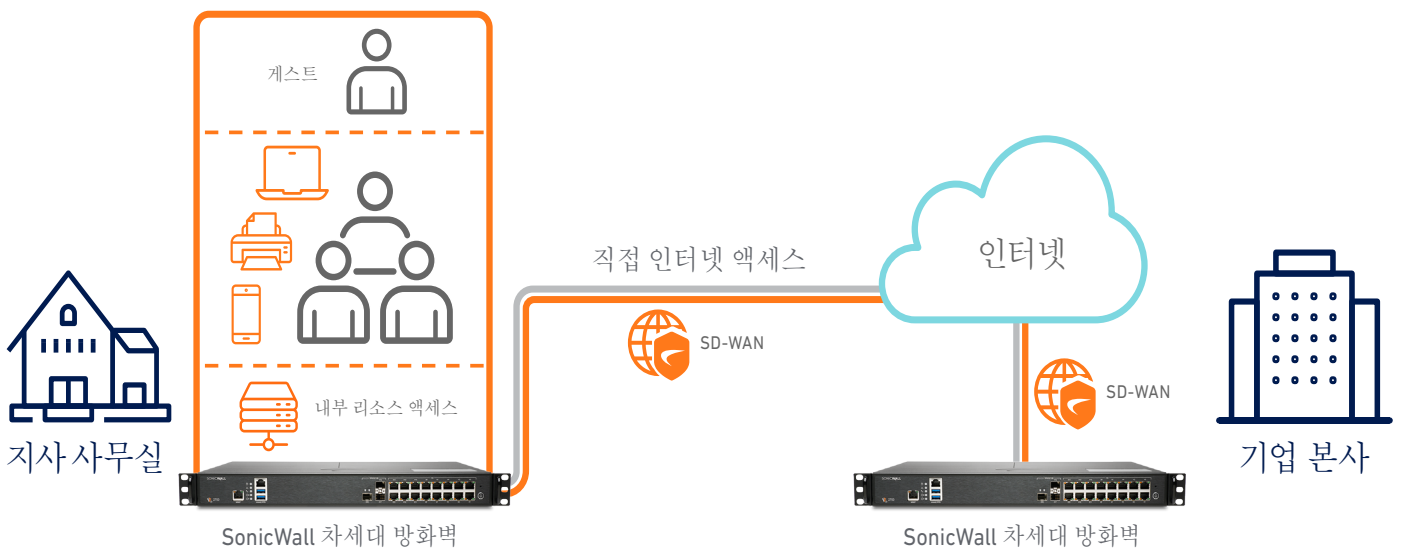


### 중간 규모 분산형 기업

SonicWall 7세대 NSa 시리즈는 SD-WAN을 지원하고 중앙집중식으로 관리할 수 있어, 중간 규모 분산형 기업에 완벽하게 적합합니다. 이 배포 옵션의 특징은 다음과 같습니다.

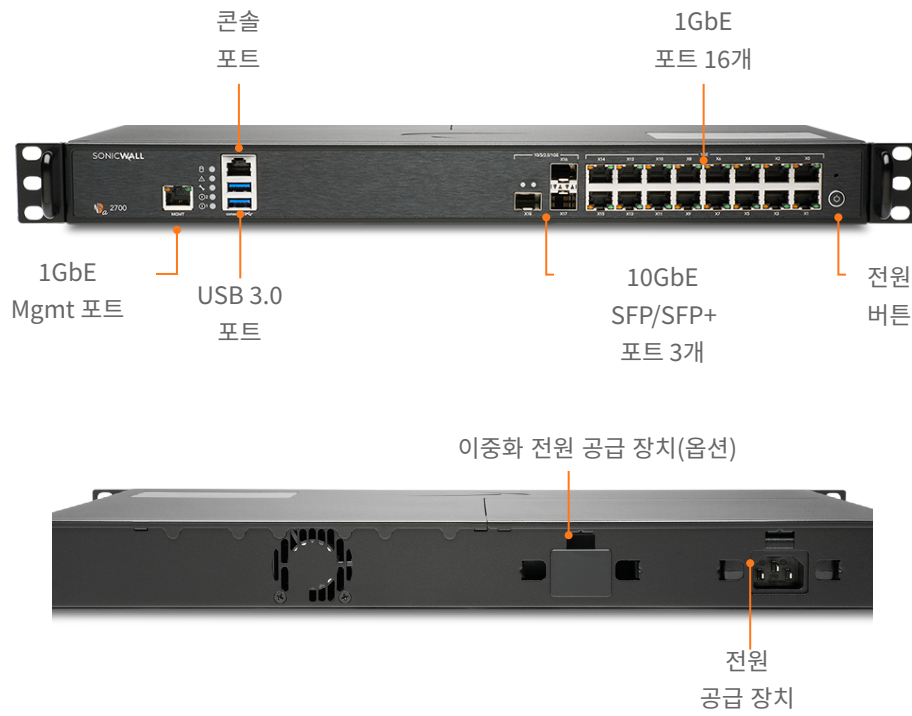
- 멀티 기가비트급 위협 분석 성능을 지닌 NGFW에 투자하여, 변화를 거듭하는 위협 환경에 대비된 확실한 미래 보장
- 기업 본사를 통한 백홀링 대신 인터넷을 통해 분산된 지사 사무실로 직접 안전하게 액세스
- 분산된 지사 사무실에서 기업 본사 또는 공용 클라우드에 저장된 내부 리소스에 안전하게 액세스하고 애플리케이션 레이턴시 대폭 단축

- TLS 1.3 등 암호화된 프로토콜을 사용하는 위협 자동 차단, 고도화된 대부분의 공격으로부터 네트워크 안전하게 보호
- 직관적인 단일 사용자 인터페이스를 통한 중앙집중식 관리 시스템으로 복잡성을 해소하고 효율 극대화
- 40GbE 및 10GbE 연결을 포함한 높은 포트 확장성으로 분산형 기업 및 광역 네트워크 지원

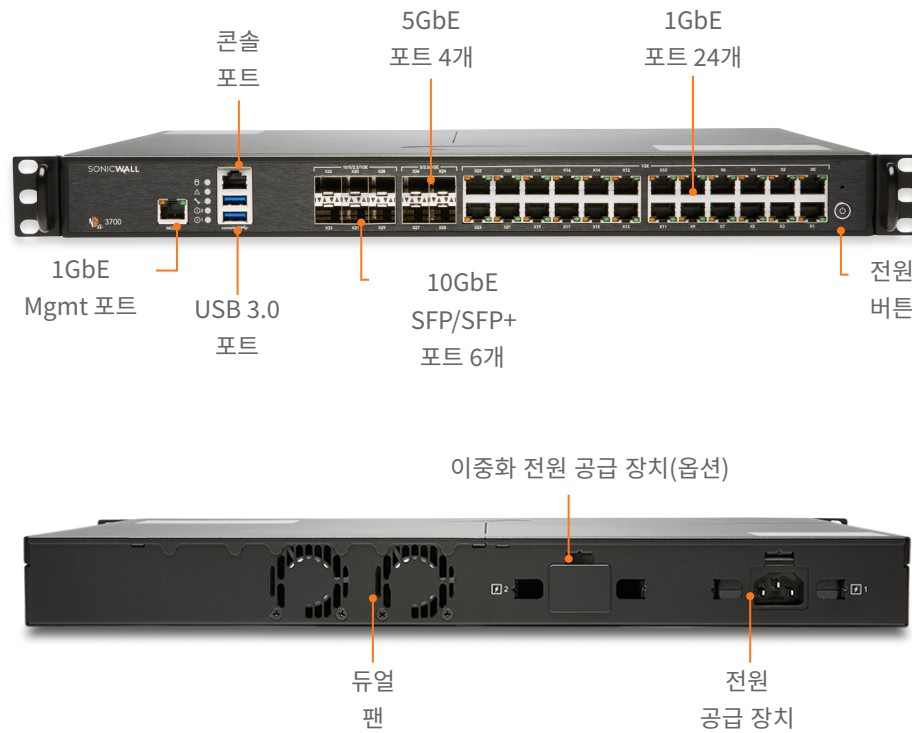


## SonicWall 7세대 NSa 시리즈

### NSa 2700

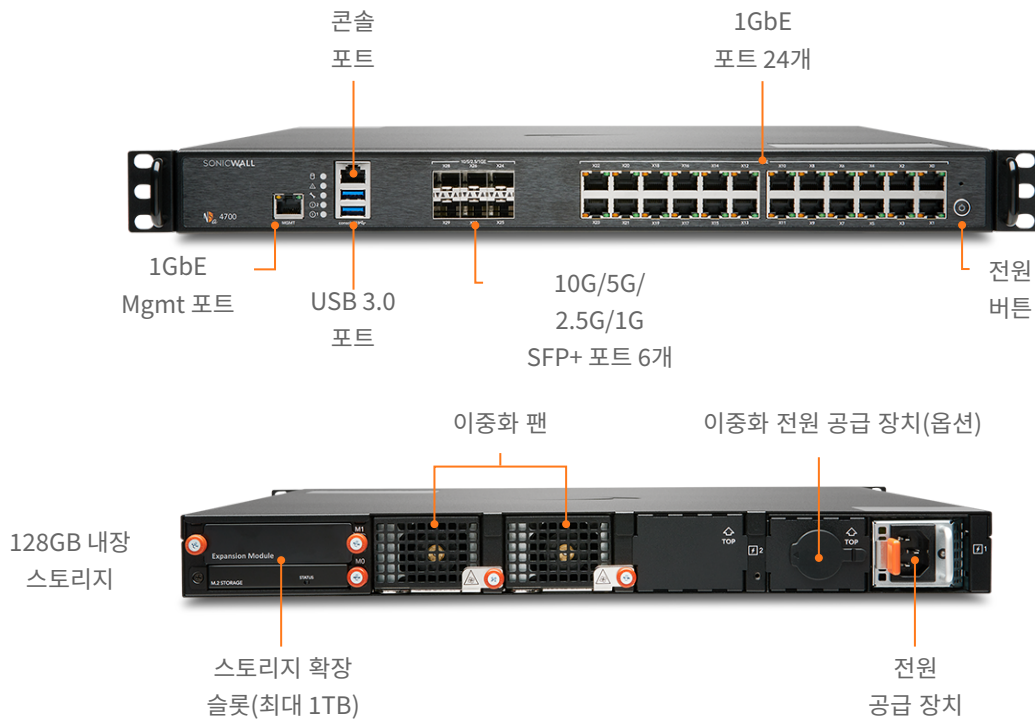


### NSa 3700

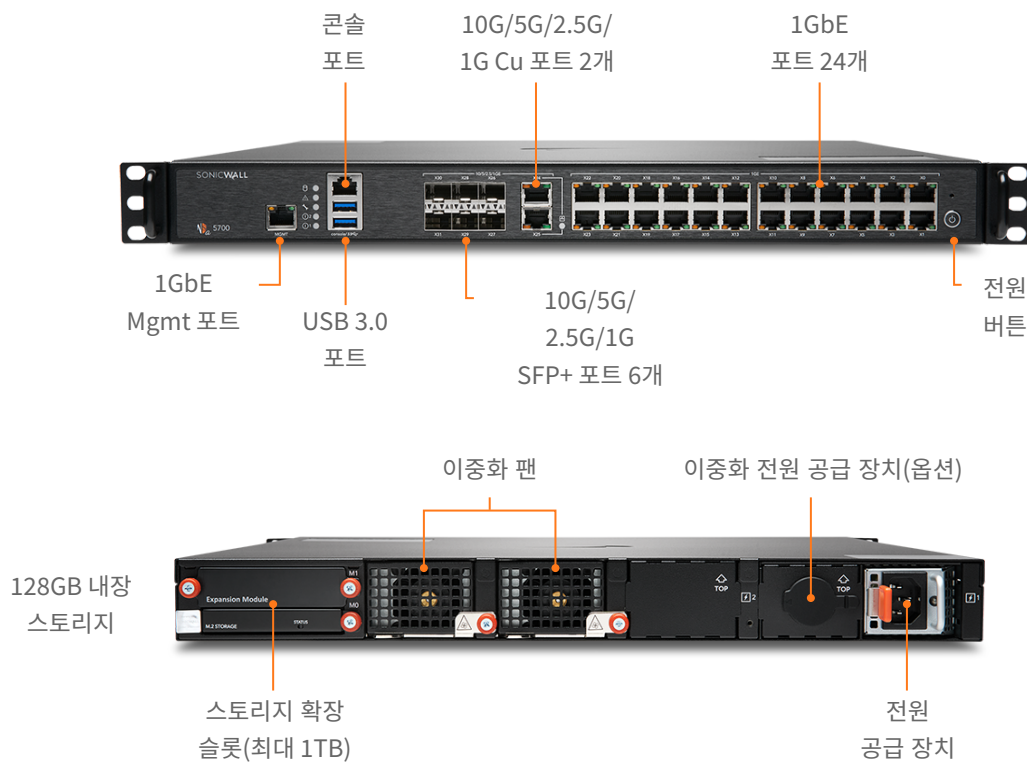


## SonicWall 7세대 NSa 시리즈

### NSa 4700



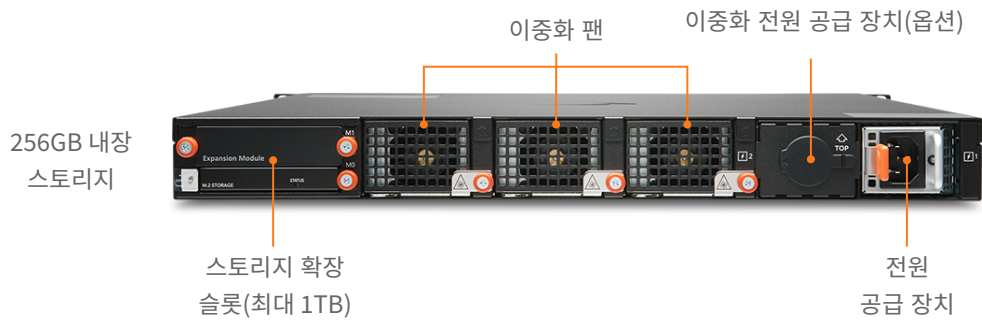
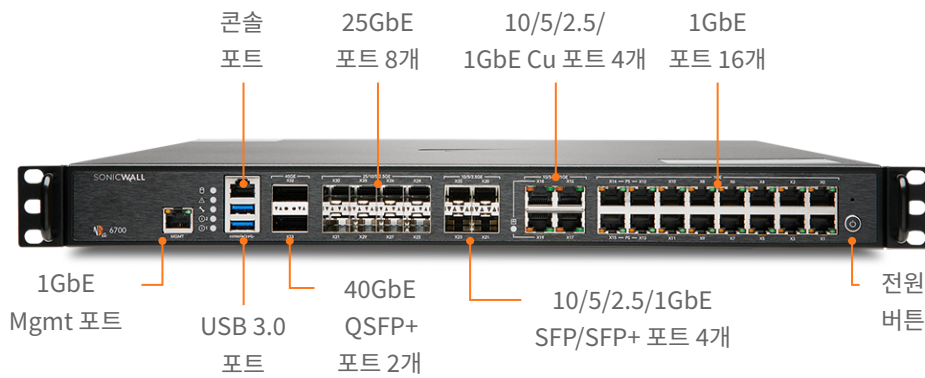
### NSa 5700





## SonicWall 7세대 NSa 시리즈

### NSa 6700



### 서비스 제공 파트너

SonicWall 솔루션의 계획, 구축, 최적화에 도움이 필요하십니까? SonicWall Advanced Services Partners는 체계적인 교육으로 세계 최고 수준의 전문 서비스를 제공합니다. 자세히 알아보기:

[www.sonicwall.com/PES](http://www.sonicwall.com/PES)

## 7세대 NSa 시리즈 시스템 사양

방화벽	NSa 2700	NSa 3700	NSa 4700	NSa 5700	NSa 6700
운영 체제	SonicOS 7				
인터페이스	1GbE 16개, 10G SFP+ 3개, USB 3.0 2개, 콘솔 1개, Mgmt 1개 포트 구성	1GbE 24개, 10G SFP+ 6개, 5G SFP+ 4개, USB 3.0 2개, 콘솔 1개, Mgmt 1개 포트 구성	10G/5G/2.5G/1G (SFP+) 6개, 1GbE Cu 24개, USB 3.0 2개, 콘솔 1개, Mgmt 1개 포트 구성	10G/5G/2.5G/1G (SFP+) 6개, 10G/5G/2.5G/1G (Cu) 2개, 1GbE Cu 24개, USB 3.0 2개, 콘솔 1개, Mgmt 1개 포트 구성	40G 2개, 25G 8개, 10G/5G/2.5G/1G SFP+ 4개, 10G/5G/2.5G/1G (Cu) 4개, 1GbE (Cu) 16개, USB 3.0 2개, 콘솔 1개, Mgmt 1개 포트 구성
스토리지	64GB M.2	128GB M.2	128GB	128GB	256GB M.2
확장	스토리지 확장 슬롯(최대 256GB)	스토리지 확장 슬롯(최대 256GB)	스토리지 확장 슬롯(최대 1TB)	스토리지 확장 슬롯(최대 1TB)	스토리지 확장 슬롯(최대 1TB)
논리적 VLAN 및 터널 인터페이스(최대)	256	256	512	512	512
SSO 사용자	40000	40000	50000	50000	70000
액세스 포인트 지원 수(최대)	512	512	512	512	512
<b>방화벽/VPN 성능</b>					
방화벽 검사 처리량 <sup>1</sup>	5.2Gbps	5.5Gbps	18Gbps	28Gbps	36Gbps
위협 방지 처리량 <sup>2</sup>	3.0Gbps	3.5Gbps	9.5Gbps	15Gbps	19Gbps
애플리케이션 검사 처리량 <sup>2</sup>	3.6Gbps	4.2Gbps	11Gbps	18Gbps	20Gbps
IPS 처리량 <sup>2</sup>	3.4Gbps	3.8Gbps	10Gbps	17Gbps	20Gbps
맬웨어 방지 검사 처리량 <sup>2</sup>	2.9Gbps	3.5Gbps	9.5Gbps	16Gbps	18.5Gbps
TLS/SSL 검사 및 복호화 처리량 (DPI SSL) <sup>2</sup>	800Mbps	850Mbps	5Gbps	7Gbps	9Gbps
IPSec VPN 처리량 <sup>3</sup>	2.10Gbps	2.2Gbps	11Gbps	15Gbps	19Gbps
초당 연결	21000	22000	115000	228000	228000
최대 연결(SPI)	1500000	2000000	4000000	5000000	8000000
최대 DPI-SSL 연결	125000	150000	350000	350000	750000
최대 연결(DPI)	500000	750000	2000000	3500000	6000000
<b>VPN</b>					
사이트간 VPN 터널	2000	3000	4000	6000	6000
IPSec VPN 클라이언트(최대)	50(1000)	50(1000)	500(3000)	2000(4000)	2000(6000)
SSL VPN 라이선스(최대)	2(500)	2(500)	2(1000)	2(1500)	2(1500)
암호화/인증	DES, 3DES, AES(128, 192, 256비트)/MD5, SHA-1, Suite B Cryptography				
키 교환	Diffie Hellman 그룹 1, 2, 5, 14v				
라우트 기반 VPN	RIP, OSPF, BGP				
인증 지원	Verisign, Thawte, Cybertrust, RSA Keon, Entrust and Microsoft CA(SonicWall-to-SonicWall VPN용), SCEP				
VPN 기능	DPD(Dead Peer Detection), DHCP 오버 VPN, IPSec NAT Traversal, 중복 VPN 게이트웨이, 라우트 기반 VPN				
Global VPN 클라이언트 플랫폼 지원	Windows 10		Microsoft® Windows Vista 32/64비트, Windows 7 32/64비트, Windows 8.0 32/64비트, Windows 8.1 32/64비트, Windows 10		
NetExtender	Windows 10 및 Linux		Microsoft Windows Vista 32/64비트, Windows 7, Windows 8.0 32/64비트, Windows 8.1 32/64비트, Mac OS X 10.4 이상, Linux FC3 이상/Ubuntu 7 이상/OpenSUSE		
모바일 연결	Apple iOS, Mac OS X, Android, Kindle Fire, Chrome OS, Windows 10		Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1(임베디드)		
<b>보안 서비스</b>					
심층 패킷 검사 서비스	게이트웨이 바이러스 백신, 스파이웨어 백신, 침입 방지, DPI SSL				
콘텐츠 필터링 서비스(CFS)	HTTP URL, HTTPS IP, 키워드 및 콘텐츠 스캐닝, ActiveX, Java, 개인정보용 쿠키, 허용/금지 목록 등 파일 유형에 따른 종합적 필터링				

## 7세대 NSa 시리즈 시스템 사양

방화벽	NSa 2700	NSa 3700	NSa 4700	NSa 5700	NSa 6700
포괄적 스펀 방지 서비스			지원됨		
애플리케이션 시각화			예		
애플리케이션 컨트롤			예		
Capture Advanced Threat Protection			예		
<b>네트워킹</b>					
IP 주소 할당	정적(DHCP, PPPoE, L2TP 및 PPTP 클라이언트), 내부 DHCP 서버, DHCP 릴레이				
NAT 모드	1:1, 1:다수, 다수:1, 다수:다수, 유연성 NAT(중복 IP), PAT, 투명 모드				
라우팅 프로토콜	BGP4, OSPF, RIPv1/v2, 정적 라우트, 정책 기반 라우팅				
QoS	대역폭 우선순위, 최대 대역폭, 보장된 대역폭, DSCP 마킹, 802.1e(WMM)				
인증	LDAP(멀티 도메인), XAUTH/RADIUS, TACACS+, SSO, Radius 어카운팅 NTLM, 내부 사용자 인터페이스, 2FA, 터미널 서비스, Citrix, 공통 액세스 카드(CAC)				
로컬 사용자 데이터베이스	1000	1000	2500	2500	3200
VoIP	Full H323-v1-5, SIP				
표준	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEE 802.3				
FIPS 140-2 규격	예	예	보류 중	보류 중	보류 중
인증	ICSA 엔터프라이즈 방화벽, ICSA 안티바이러스, IPv6/USGv6				
인증(진행 중)	국제공통평가기준 NDPP 방화벽, VPN 및 IPS 포함				
공통 액세스 카드(CAC)	지원됨				
고가용성	액티브/패시브, 상태 기반 동기화 포함				
<b>하드웨어</b>					
폼 팩터	1U 랙 장착 가능				
팬	1	2	2개(탈착 가능)	2개(탈착 가능)	3개(탈착 가능)
전원 공급 장치	60W	90W	350W	350W	350W
최대 소비 전력(W)	21.5	36.3	108.1	128.1	139.2
이중화 전원 공급 장치	100~240V AC, 50~60Hz				
총 열 방출량	73.32 BTU	123.78 BTU	368.62 BTU	436.82 BTU	474.67 BTU
치수	43 x 32.5 x 4.5cm 16.9 x 12.8 x 1.8in	43 x 32.5 x 4.5cm 16.9 x 12.8 x 1.8in	43 x 46.5 x 4.5cm 16.9 x 18.1 x 1.8in	43 x 46.5 x 4.5cm 16.9 x 18.1 x 1.8in	43 x 46.5 x 4.5cm 16.9 x 18.1 x 1.8in
중량	4.0kg / 8.8lbs	4.6kg / 10.2lbs	7.8kg	7.8kg	8.1kg
WEEE 중량	4.2kg / 9.3lbs	4.8kg / 10.6lbs	9.6kg	9.6kg	9.9kg
적재 중량	6.4kg / 14.1lbs	7kg / 15.4lbs	13.5kg	13.5kg	13.8kg
환경(작동/보관)	32°~105°F (0°~40°C) / -40°~158°F (-40°~70°C)				
습도	5~95% 비응축	5~95% 비응축	0~90% R H 비응축	0~90% R H 비응축	0~90% R H 비응축
<b>규제</b>					
규제 모델 번호	1RK51-109	1RK52-110	1RK53-115	1RK53-116	1RK54-118
주요 컴플라이언스 규제	FCC Class A, CE(EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, ANATEL, BSMI				

<sup>1</sup> 테스트 방법은 RFC 2544(방화벽용)에 따른 최대 성능. 실제 성능은 네트워크 조건 및 활성화된 서비스에 따라 다를 수 있음.

<sup>2</sup> 위험 방지/게이트웨이 안티바이러스/안티스파이웨어/업계 표준 Keysight HTTP 성능 테스트 도구를 사용해 측정된 IPS 처리량. 다수의 포트 쌍을 통해 다중 흐름으로 수행된 테스트. 게이트웨이 안티바이러스, 안티스파이웨어, IPS 및 애플리케이션 컨트롤을 활성화한 상태로 측정된 위험 방지 처리량.

<sup>3</sup> RFC 2544를 준수하여 패킷 사이즈가 1,418바이트인 AESGMAC16-256 암호화를 UDP 트래픽을 사용해 측정된 VPN 처리량. 모든 사양, 기능 및 가용성은 변경될 수 있음.



## SonicOS 7.0 기능 요약

### 방화벽

- 상태 기반 패킷 검사
- 비재조립 심층 패킷 검사
- DDoS 공격 보호(UDP/ICMP/SYN 플러드)
- IPv4/IPv6 지원
- 원격 액세스를 위한 생체 인증
- DNS 프록시
- 전체기능 API 지원
- SonicWall Switch 통합
- SonicWall Wi-Fi 6 AP 통합
- SD-WAN 확장성
- SD-WAN Usability Wizard<sup>1</sup>
- 연결 확장성(SPI, DPI, DPI SSL)
- 향상된 대시보드<sup>1</sup>
- 향상된 장치 보기
- 최상위 트래픽 및 사용자 요약
- 위협 인사이트
- 알람 센터

### TLS/SSL/SSH 복호화 및 검사

- 향상된 보안 기능의 TLS 1.3<sup>1</sup>
- TLS/SSL/SSH를 위한 심층 패킷 검사
- 객체, 그룹 또는 호스트 이름의 포함/제외
- SSL 컨트롤
- CFS를 통한 DPI-SSL 개선 사항
- Zone 또는 정책 별 세부 DPI-SSL 컨트롤
- Capture 첨단 위협 보호 기능<sup>2</sup>
- 실시간 심층 메모리 검사
- 클라우드 기반 멀티 엔진 분석<sup>2</sup>
- 가상 샌드박스
- 하이퍼바이저 레벨 분석
- 전체 시스템 에뮬레이션
- 광범위한 파일 유형 검사
- 자동 및 수동 제출
- 실시간 위협 분석 인텔리전스 업데이트<sup>2</sup>
- 분석중 차단
- Capture Client<sup>2</sup>

### IPS<sup>2</sup>

- 시그니처 기반 스캐닝
- Aruba ClearPass와 네트워크 액세스 제어 통합
- 자동 시그니처 업데이트
- 양방향 검사
- 세부적 IPS 규칙 기능
- GeoIP 실행
- 동적 목록을 사용한 봇넷 필터링
- 정규식 매칭

### 안티맬웨어<sup>2</sup>

- 스트림 기반 맬웨어 스캐닝
- 게이트웨이 바이러스 백신
- 게이트웨이 안티스파이웨어
- 양방향 검사
- 파일 크기 무제한
- 클라우드 맬웨어

### 애플리케이션 식별<sup>2</sup>

- 애플리케이션 컨트롤
- 애플리케이션 대역폭 관리
- 커스텀 애플리케이션 시그니처 생성
- 데이터 유출 방지
- NetFlow/IPFIX를 통한 애플리케이션 리포팅
- 종합적인 애플리케이션 시그니처 데이터베이스

### 트래픽 가시화 및 분석

- 사용자 활동
- 애플리케이션/대역폭/위협 사용
- 클라우드 기반 분석

### HTTP/HTTPS 웹 콘텐츠 필터링<sup>2</sup>

- URL 필터링
- 프록시 우회
- 키워드 차단
- 평판 기반의 콘텐츠 필터링 서비스(CFS 5.0)
- DNS 필터링
- 정책 기반 필터링(제외/포함)
- HTTP 헤더 삽입
- 대역폭 관리 CFS 등급 카테고리
- 통합형 정책 모델, 앱 컨트롤 포함
- 콘텐츠 필터링 클라이언트

### VPN

- 보안 SD-WAN
- 자동 설정 VPN
- 사이트간 연결을 위한 IPSec VPN
- SSL VPN 및 IPSec 클라이언트 원격 액세스
- 이중화 VPN 게이트웨이
- iOS, Mac OS X, Windows, Chrome, Android 및 Kindle Fire를 위한 모바일 연결
- 라우트 기반 VPN(OSPF, RIP, BGP)

### 네트워킹

- PortShield
- 점보 프레임
- 경로상 MTU 조정
- 강화된 로깅
- VLAN 트렁킹
- 포트 미러링(SonicWall Switch)
- Layer-2 QoS
- 포트 보안
- 동적 라우팅(RIP/OSPF/BGP)
- SonicWall 무선 컨트롤러
- 정책 기반 라우팅(ToS/지표 및 ECMP)
- NAT
- DHCP 서버
- 대역폭 관리
- 상태 동기화를 통한 A/P 고가용성
- 인바운드/아웃바운드 로드 밸런싱
- 고가용성 - 상태 동기화를 통한 활성/대기
- L2 브리지, 유선/가상 유선 모드, 탭 모드, NAT 모드
- 비대칭 라우팅
- 공통 액세스 카드(CAC) 지원

### VoIP

- 세부 QoS 제어
- 대역폭 관리
- VoIP 트래픽을 위한 DPI
- H.323 게이트 키퍼 및 SIP 프록시 지원

### 관리, 모니터링 및 지원

- Capture Security 어플라이언스(CSa) 지원
- Capture Threat Assessment(CTA) v2.0
- 새로운 설계 또는 템플릿
- 업계 및 글로벌 평균 비교
- 새로운 UI/UX, 직관적인 기능 레이아웃<sup>1</sup>
- 대시보드
- 장치 정보, 애플리케이션, 위협
- 토폴로지 보기
- 간편한 정책 생성 및 관리
- 정책/객체 사용 통계<sup>1</sup>
- 사용 vs 미사용
- 활성 vs 비활성
- 정적 데이터에 대한 글로벌 검색
- 스토리지 지원<sup>1</sup>

## SonicOS 7.0 기능 요약

### 관리, 모니터링 및 지원

- 내부 및 외부 스토리지 관리<sup>1</sup>
- WWAN USB 카드 지원(5G/LTE/4G/3G)
- 네트워크 보안 관리자(NSM) 지원
- 웹 GUI
- 명령행 인터페이스(CLI)
- 제로 터치 등록 및 권한설정
- CSC 간편 보고 기능<sup>1</sup>
- SonicExpress 모바일 앱 지원
- SNMPv2/v3
- SonicWall GMS(Global Management System)<sup>2</sup>를 통한 중앙 집중식 관리 및 보고
- 보고 및 분석용 API
- 로깅
- Netflow/IPFix 내보내기
- 클라우드 기반 설정 백업
- BlueCoat 보안 분석 플랫폼
- 애플리케이션 및 대역폭 가시화
- IPv4 및 IPv6 관리
- CD 관리 스크린
- 캐스케이드 스위치를 포함한 Dell N-Series 및 X-Series 스위치 관리

### 디버깅 및 진단

- 향상된 패킷 모니터링
- UI의 SSH 터미널

### 무선

- SonicWave AP 클라우드 및 방화벽 관리
- WIDS/WIPS
- Rogue AP 방지
- 빠른 로밍(802.11k/r/v)
- 802.11s 메쉬 네트워킹
- 자동 채널 선택
- RF 스펙트럼 분석
- 평면도 보기
- 토폴로지 보기
- 대역 조정
- 빔포밍
- 전파 점유 시간 공정성
- 블루투스 LE
- MiFi 익스텐더
- RF 향상 및 개선 사항
- 게스트 주기적 할당

<sup>1</sup>SonicOS 7.0에서 이용 가능한 새로운 기능

<sup>2</sup>추가 구독 필요

## SonicWall 7세대 NSa 시리즈 자세히 알아보기

[www.sonicwall.com/products/firewalls](http://www.sonicwall.com/products/firewalls)

### SonicWall 소개

SonicWall은 초분산 시대와 모든 사람이 원격, 모바일 및 비보안 상태인 업무 현실을 위한 안정적이고 확장 가능하며 매끄러운 사이버 보안을 제공합니다. SonicWall은 알려지지 않은 정보에 대한 실시간 가시성을 제공하며 혁신적인 경제성으로 전 세계 기업, 정부, 중소기업 간 사이버 보안 비즈니스 격차를 해소합니다. 자세한 정보는 [www.sonicwall.com](http://www.sonicwall.com)을 방문하십시오.



#### SonicWall Inc.

1033 McCarthy Boulevard | Milpitas, CA 95035

기타 정보는 웹 사이트에서 확인할 수 있습니다.

[www.sonicwall.com](http://www.sonicwall.com)

SONICWALL®

© 2023 SonicWall Inc. 모든 권리 보유.

SonicWall은 미국 및/또는 기타 국가에서 SonicWall Inc. 및/또는 그 계열사의 상표 또는 등록상표입니다. 그 밖의 모든 상표와 등록상표는 각 소유권자의 재산입니다. 본 문서의 정보는 SonicWall Inc. 및/또는 그 계열사의 제품과 관련된 정보입니다. 본 문서에 의해서 또는 SonicWall 제품 판매와 연계하여 금반언의 원칙 또는 기타의 방법으로 명시적으로든 암묵적으로든 일체의 지적재산권에 대해 어떠한 라이선스도 부여되지 않습니다. 본 제품의 라이선스 계약에 명시된 바와 같이 계약 조건에 명시된 바를 제외하고, SonicWall 및/또는 그 계열사는 상품성, 특정 목적에 대한 적합성 또는 비침해에 대한 암묵적 보증(이에만 국한되지 않음) 등을 포함하여 제품과 관련된 명시적, 암묵적 또는 법적 보증을 부인합니다. SonicWall 및/또는 그 계열사는 어떤 경우에도 본 문서의 이용 또는 이용하지 못함으로 인해 생겨나는 직접적, 간접적, 결과적, 징벌적, 특별 손해 또는 부수적 손해(이익 상실, 사업 중단 또는 정보 손실로 인한 피해를 포함하되 이에만 국한되지 않음)에 대해, 비록 SonicWall 및/또는 그 계열사가 그 피해의 가능성을 숙지하고 있었다 하더라도 법적 책임을 지지 않습니다. SonicWall 및/또는 그 계열사는 본 문서의 내용에 대해 정확성이나 완전성에 관하여 어떤 진술이나 보증도 하지 않으며, 통지 없이 언제든지 명세서와 제품 설명을 변경할 권리가 있습니다. SonicWall 및/또는 그 계열사는 본 문서에 포함된 정보를 업데이트함을 약속하지 않습니다.